IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA
HUNTINGTON

IN THE MATTER OF THE SEARCH OF THE BLACK AND SILVER IPHONE, CURRENTLY LOCATED AT 300 SUMMERS STREET, CHARLESTON, WV 25301	Case No. 3:21-mj-00060

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Terry Hedrick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Secret Service (hereinafter, the "USSS"), Charleston, WV Resident Office, and have been so employed since December of 2004. I am authorized, pursuant to 18 U.S.C. § 3056(b), to detect and arrest any person who violates any of the laws of the United States relating to electronic fund transfer frauds, access device frauds, false identification documents or devices, and any fraud or criminal or unlawful activity or against any federally insured financial institution. Additionally, I am authorized, pursuant to 18 U.S.C. § 3056(c), to execute warrants issued under the laws of the United States.

3. Since becoming a Secret Service Special Agent, I have personally investigated

and/or assisted in investigations relating to violations of the laws of the United States relating to financial crimes, including romance frauds and other online schemes, specifically 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. §§ 1956-57 (money laundering) and 18 US.C. 2315 (receipt of stolen property). I received 30 weeks of training at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, and at the Secret Service's Rowley Training Center in Beltsville, Maryland, before my assignment as a Secret Service Special Agent in the Charleston, WV Resident Office.

4. As a Special Agent with the USSS, I have been involved in other financial elder abuse and romance fraud investigations. I know from my training and experience that those persons involved in committing those types of crimes spend a great deal of time each week seeking out potential victims through email, text messages, and social media websites such as Google Hangouts, Go Fish, Plenty of Fish and various other dating sites. I also know that people who commit these crimes stay in constant contact with victims, creating a friendship that ultimately leads to a false romantic relationship with victims. I know that these fraudsters tell their victims untrue stories about their employment, their personal life, their family life and their need for financial assistance. In many of these instances, the fraudsters propose marriage to the victim. I know that after this romance flourishes, the fraudsters then ask victims to send them money for various reasons. Some of the fraudsters' reasons include family medical emergencies, or because the fraudsters need to pay their oil rig workers, or need money to ship gold or other valuables back to the United States to be allegedly shared with the victims or finally, for bail when the fraudsters were allegedly arrested after leaving a foreign country.

5. I know from my training and experience that these fraudsters instruct their victims to send large amounts of currency through the U.S. Mail, FedEx, and the United Parcel Service

(UPS). I know that these fraudsters get their victims to send money to them via cashier checks, personal checks, money orders, wire transfers, bitcoin and through many different mobile payment processing companies. These mobile payment processing companies include Transferwise, Ping Express, Money Gram, Western Union, Walmart, Pay Pal, Square, Cash App, Xoom, Zelle, and others.

6. The statements in this Affidavit are based in part on information provided by other investigators, law enforcement officers, witnesses, records obtained through investigation, as well as training and experience and my own investigation of this matter. This ongoing investigation is financial in nature, thus any figures I cite in this Affidavit are based on calculations and tracing conducted to date and may be revised later. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each fact known to me concerning this investigation.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

7. The property to be searched is a black and silver iPhone, hereinafter the "Device." The Device is currently located at the Secret Service's Office located at 300 Summers Street, Charleston, WV 25301.

8. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. Based on the facts set forth in this affidavit, there is probable cause to believe that Abdul Inusah (INUSAH) has violated 18 U.S.C. § 1343 and 18 U.S.C. § 2315. INUSAH

was indicted for violations of 18 U.S.C. § 1343 and 18 U.S.C. § 2315 on April 28, 2021 (hereinafter, the "Indictment"), and was the subject of an arrest warrant issued for him on that same date, 3:21-cr-00070.

10. INUSAH was involved with various online schemes, including romance fraud scams, in which he or his associates created false online personas which contacted victims and created relationships with these victims, specifically, Victim T.G., Victim M.C., and Victim G.W (collectively, the "romance fraud victims.") Each of the romance fraud victims informed investigators that they met Grace, Miarama and Judith through online dating websites and social media.

11. Victim G.W. interviewed by investigators and relayed that he had often communicated with the individual that he knew as Grace Benson ("Grace") through Google Hangouts or telephone calls. Similarly, Victim M.C. informed investigators during his interview that he communicated frequently with the individual that he knew as Miarama Ousman ("Miarama") through text messages. Victim T.G. also told investigators that he frequently communicated with the individual he knew as Judith Wimmer ("Judith") through texts and emails.

12. As detailed in the Indictment, the romance fraud victims all sent money to bank accounts under INUSAH's control.

13. Furthermore, from investigators' review of INUSAH's financial records showed that INUSAH used mobile check deposit feature to deposit checks into his bank account and Zelle to transfer funds.

14. Users are generally able to use a bank's mobile check feature by using a mobile device to take a picture of a check and then enter that check's information into the user's bank account.

15. Zelle is a digital payment network and part of a private financial services company owned by Bank of America, BB&T now "Truist," Capital One, J.P. Morgan Chase N.A., PNC Bank, U.S. Bank and Wells Fargo. Zelle allows an individual to electronically transfer money from his or her bank account to another registered user's bank account, held within the United States, by using a mobile device or the website of a participating bank institution.

16. INUSAH's use of Zelle and mobile check deposit shows that INUSAH used online banking. In my training and experience, individuals are able to use smartphones like the Device to access their bank accounts online.

17. The romance fraud victims' statements to investigators that they communicated with Grace, Judith and Miarama through text messages, emails, Google Hangouts and phone calls, shows that phones, including smartphones such as the Device, were instrumental to committing the wire fraud scheme that INUSAH was involved in. Smartphones such as the Device often retain evidence of old text messages, emails and call logs.

Financial Analysis

18. A review of INUSAH's known bank accounts shows that he received wires or other deposits from at least 9 different individuals currently believed to be fraud victims, which total to approximately $161,125.00 at this time. However, as the financial breakdown below

shows, INUSAH is believed to have received a much greater sum of fraud proceeds through cash deposits, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. INUSAH had reported wages totaling $15,691.40 from March 30, 2019 through March 30, 2020. INUSAH has no reported wages for the first quarter of 2021.

Deposits Received from Victims	$161,125.00
Cash Deposits	$61,401.00
Deposits from Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$146,076.67
Total Illegal Proceeds Received by INUSAH	**$368,602.67**

19. As stated earlier in this Affidavit, several other individuals associated with INUSAH were also indicted on April 28, 2021, two of these individuals were named Kenneth Emeni and Kenneth Ogudu. Investigators review of financial records have found several financial transactions that link INUSAH to Kenneth Emeni and Kenneth Ogudu. Examples of Zelle transfers between Kenneth Emeni, Kenneth Ogudu and INUSAH are detailed below:

Date	Sender	Amount	Recipient
3/8/19	Kenneth Emeni	$100	INUSAH
3/19/19	Kenneth Emeni	$100	INUSAH
3/21/19	Kenneth Emeni	$200	INUSAH
4/25/19	Kenneth Emeni	$1,000	INUSAH
8/10/19	Kenneth Ogudu	$600	INUSAH

9/7/19	INUSAH	$120	Kenneth Ogudu
9/21/19	INUSAH	$200	Kenneth Ogudu

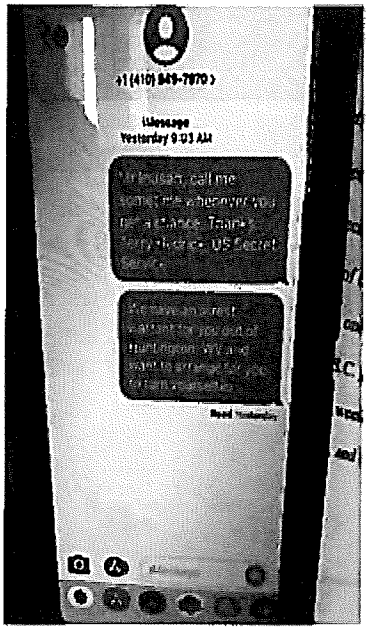
Law Enforcement's Communication with INUSAH via the Device

20. Law enforcement believes that the Device is assigned cellular number (410) 949-7970. I texted INUSAH at the (410) 494-7970 number on May 26, 2021.

21. After I texted the Device, I received a call from a Huntington attorney who claimed that INUSAH had contacted him seek representation but, that the Huntington attorney did not generally undertake federal criminal work and would be referring INUSAH to one of his associates.

22. I was then contacted by another Huntington lawyer who claimed that he was considering representing INUSAH, but I later learned that the second Huntington lawyer later declined to represent INUSAH.

23. Based on the contact from the Huntington lawyers and the fact that my text was "read" by the user of the Device as shown by the read receipt of the text message below, there is probable cause to believe that INUSAH is the user of the Device.



24. On June 10, 2021, I received a phone call from INUSAH on the Device. During the phone call, I again informed INUSAH there was a warrant for his arrest and that he needed to turn himself into authorities. INUSAH told me that he had seen the "paperwork" and that his name was not on it.

25. Based on my training and experience, I believe that INUSAH was referring an indictment – possibly the indictment against Kenneth Emeni et al (*see* 3:21-cr-00068) - when he stated that he had seen the "paperwork." Moreover, based on my training and experience, I believe that INUSAH could have only seen the "paperwork" he referenced was by looking by searching court records or news stories involving the indictments online or by talking to co-conspirators.

26. INUSAH also told me he was in Rhode Island and asked if he could fly to West Virginia to turn himself into authorities during our phone conversation.

27. The Secret Service had previously obtained a search warrant for the Device's geolocation data (hereinafter, the "geolocation warrant."). United States Magistrate Judge Cheryl A. Eifert signed the geolocation warrant on June 1, 2021. *See* 3:21-mj-00055. Investigators' review of the geolocation data shows that INUSAH was not located in Rhode Island on June 10, 2021 but was in fact located near Charleston, West Virginia during the time of our phone call.

28. INUSAH was arrested by the Secret Service on the morning of June 16, 2021. I transported INUSAH from the Charleston area to the federal courthouse in Huntington, West Virginia. During our car trip, INUSAH informed another Secret Service Task Force Officer that he was had heard "Kenny got picked up."

29. Based on my training and experience, INUSAH's comment that he heard "Kenny got picked up" shows that there is probable cause to believe that he is communicating with others who may be co-conspirators or witnesses to his and others' crimes.

30. As users are able to use the Device to send and receive text messages and calls, there may be evidence of INUSAH's communications with his co-conspirators and other witnesses – both during the time period spanning his criminal activities and the time period after which he knew there was a federal arrest warrant issued for him but before he was arrest.

31. The Device is currently in the lawful possession of the Secret Service. It came into the Secret Service's possession in the following way by being seized incident to INUSAH's arrest. Therefore, while the Secret Service might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain

that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

32. When INUSAH was arrested he had two phones in his possession, a blue flip phone and the Device.

33. In my training and experience, it is common for individuals engaging in illegal activities often maintain multiple electronic devices. It is often common for individuals engaging in illegal activities to contact victims or co-conspirators from a different electronic device than an electronic device that they use for legitimate and everyday activities.

34. The Device is currently in storage at the Secret Service's Office located at 300 Summers Street, Charleston, WV 25301. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Secret Service.

TECHNICAL TERMS

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call

log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other

digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication

devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

36. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

37. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

h. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

i. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

j. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

k. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

l. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

m. I know that when an individual uses an electronic device to communicate with victims through electronic devices or engage in financial transactions in furtherance of the fraud over the Internet, the individual's electronic device will

generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

40. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

41. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

TERRY HEDRICK
SPECIAL AGENT
UNITED STATES SECRET SERVICE

Subscribed and sworn-to by the Affiant telephonically in accordance with the procedures of Rule 4.1 of the Federal Rules of Criminal Procedure, on June 17, 2021.

CHERYL A. EIFERT
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA